Int. J. Advanced Networking and Applications
Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

Data Security through Node-Disjoint on Demand Multipath Routing in MANETs

Y. Vasudeva Reddy
Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool, India.
yvr.gpr@gmail.com
Dr. M. Nagendra
Professor, Head of the Department, Department of Computer Science and Technology, Sri Krishnadevaraya University, Ananthapuramu, India.
nagendra_m@rediff.com

Abstract

Mobile Ad Hoc Networks(MANETs) are the wireless networks which can be deployed instantly without requiring any fixed wired infrastructure. MANETs are specifically very much useful in military, commercial and civilian applications. Since infrastructure less MANETs have dynamic topology and battery powered mobile nodes, it is a challenging task to provide secure data transmission between any pair of nodes in MANET. Multipath on Demand Routing is one possible solution to provide security in MANET. This paper proposes a new method (DSNMR) of providing secure communication by integrating trust based mechanism with multipath on demand routing approaches in MANETs. The simulation analysis of proposed method reveals the facts that the method provides significant security to the data compared to previous related work.

Keywords: **Data Security, Mobile Ad Hoc Networks, Multipath Routing, Node-disjoint, Protocol Design.**

Date of Submission: Mar 13, 2019 Date of Acceptance: Apr 13, 2019

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are popular due to their rapid deployment as and when there is a need of infrastructure less temporary complete wireless network [1]–[3], [49].As shown in Fig.1, MANET is a multi-hop wireless network in which the nodes act as both hosts and routers i.e., nodes forward the packets of other nodes which present between source and destination hosts. Routing is an important networking function which finds the routes between source and destination nodes before data transmission takes place between them. The nodes in MANETs are moving constantly from one location to another and it results in dynamic topology of MANET. Moreover, the nodes are constrained by their battery power. Hence, facilitating routing in MANETs is a challenging task.

All the routing protocols of MANET can be classified into three categories: proactive (static), reactive (on-demand) and hybrid protocols [4]. Proactive routing protocols like DSDV[5], WRP[6], CGSR[7], GSR[8], etc. establish routing paths between each pair of nodes in MANET before data transmission takes place. To maintain the routes according to the changes in network topology, the nodes periodically exchange topology information which is an overhead in proactive routing approach. Reactive routing protocols as ABR [9], TORA [10], DSR [11], AODV [12], etc., discover the route only when there is data transmission between a pair of nodes. Moreover, the routes are maintained as long as data transmission takes place. Once the data transmission is completed, the route is no more maintained. Reactive routing protocols discover the routes using query-reply based approach. Hybrid routing protocols like ZRP [13]are developed using merits of both static and dynamic routing protocols. Irrespective of type of routing protocol used in MANET, there exist some common and/or specific routing attacks [14]–[20]. Also, several solutions to solve security problems in MANETs have been proposed. One possible solution is to use multipath routing instead of traditional unipath routing in MANET.

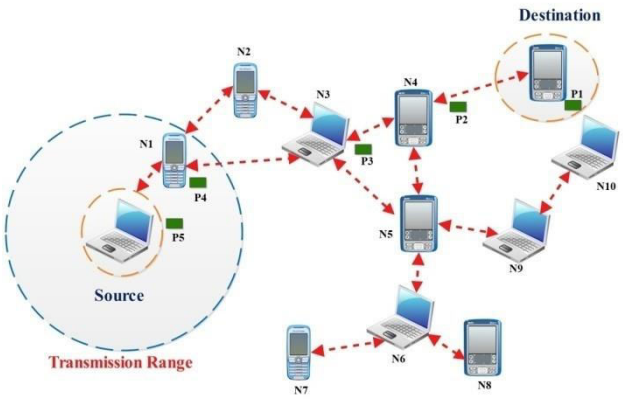

Figure 1. Mobile Ad Hoc Network

Another classification of MANET routing protocols is based on number of paths used for data transmission: unipath and multipath routing protocols. Only one route is used for sending data from source node to destination node in case of unipath routing. On the other hand, atleast two different routing paths are used for data transmission between source and destination nodes if multipath routing scheme is used. Multipath routing schemes provide more security than unipath routing schemes because an attacker has to compromise at least one node in each path to collapse the security system of MANET. Multipath routing protocols are two types: node-disjoint and link-disjoint protocols. No two paths must have a common

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

node in node-disjoint routing. Similarly, no common link is present between two or more paths in link-disjoint multipath routing protocols.Some of the node-disjoint protocols are [21]–[23] and a few link-disjoint protocols are [24], [25]. For security purposes, node-disjoint multipath routing protocols are preferable than link-disjoint multipath routing protocols because if the attacker destroys the common link then multiple paths will be affected in link-disjoint multipath routing protocols. Node-disjoint multipath routing protocols are also considered as link-disjoint multipath routing protocols but not vice versa. The proposed secure method, DSNMR (Data Security through Node-disjoint Multipath Routing protocol), is based on node-disjoint on-demand multipath routing scheme.

Many different protocols of security through multipath routing[26]–[34]exist in the literature. It is observed from the in-depth analysis of literature that most of the protocols were proposed to follow trust based security measurements to maintain multiple paths. A little work as [42] is providing both route security and data security. But unable to address attacks by selfish nodes which drop the data packets to save their battery power. Moreover, node mobility is also not considered in the mentioned previous work. If a highly mobile node is present in a path, then there exist more chances for route failure as the node may move away from path. With this motivation, this proposesa protocolDSNMRthat provides security in the discovery of all distinct node-disjoint multiple paths from source to destination and also during the data transmission between them. Unlike previous work, DSNMR predicts the remaining battery power levels of nodes in addition to packet drop ratio and accordingly it chooses the routes to send the data. Also, DSNMR considers node mobility factor while calculating node trust value such that a highly mobile node is trusted a little as it might move away from the path. The general framework of the proposed secure work provides flexibility in extending the work with any trust model.

This paper content is organized as follows:motivating literature work is discussed in section 2 and the mathematical model of proposed work DSNMR is presented in section 3.DSNMR evaluation is analysed in section 4 and the paper ends with conclusion in section 5.

II. RELATED WORK

Since one of the important applications of Mobile Ad hoc Networks is military communications, secure transmission of data obtained significant attention by the research community. Most of the researchers suggested to use multipath routing schemes to achieve load balancing and security in MANET. Specifically, node-disjoint on-demand multipath routing protocols are recommended by researchers [17]–[20], [35]–[37].

There exist various types of security attacks in MANETs and our previous work [38] presents a detailed survey analysis on it.It is hard to detect internal malicious nodes participating in DoS attacks. However, multipath routing schemes are most securable than unipath routing protocols in controlling DoS attacks and minimizing the data loss.

The SRP protocol proposed in [39] uses symmetric cryptographic method to secure route discovery process of on-demand routing protocols but unable to discover all existing node-disjoint multiple paths that exist between source and destination nodes in MANET. The protocol in [40] discovers all distinct node-disjoint multiple paths with certain hop count between nodes but route request messages cause delay in processing. SecMR protocol in [41] solves the limitations of [39] and [40] such that it discovers all distinct node-disjoint multiple paths with certain maximum hop count and no additional delay than normal operation of on-demand routing protocol. SecMR protocol protects the route discovery process from malicious nodes but data security is not addressed. All these work [39-41] protect the MANET from DoS attacks by malicious nodes by securing the multipath routes discovery process. Some nodes in MANET intentionally drop the data packets for saving their battery power or other reasons. These kinds of selfish nodes are difficult to be detected by the security system. The work [39-41] cannot address this attack. Our work is inspired from [41] but we address the problem of data security from selfish nodes after route discovery process.

For data security purpose, our protocol integrates a trust based security scheme with the asymmetric cryptography scheme used in multipath route discovery process. There exist different schemes of trust based security models [29], [30], [33], [34] in the literature which differ in node trust metrics used in process and all these work discover securable node-disjoint multiple paths and also not addressing data security during transmission. But out protocol uses trust based metrics for data security purpose and not to discover the paths. Clearly, the proposed work in this paper uses asymmetric cryptographic principles to protect route discovery process and route maintenance. During data transmission after the route discovery process, the proposed protocol, DSNMR, uses trust based metrics to control data loss due to selfish node attacks.Most recent work which is more relevant to our work is presented in [42] but that work used trust based route discovery process followed by cryptographic based data security. Moreover, it is mentioned that the trust value of each node is calculated as a discrete value of either 0 or 1. All the previous work mentioned in the paper, did not address the attacks by selfish nodes which drop the data packets to save their battery power. With this motivation, our proposed protocol DSNMR, calculates trust value for each node based on number of packets received and forwarded. Unlike previous work, DSNMR predicts the nodes remaining battery power levels and accordingly decide the amount of data to transmit through the paths. DSNMR assumes that the nodes with low battery level have high probability to drop the data packets and so DSNMR decreases the number of data packets through the path that have low battery power. Also, DSNMR calculates node mobility factor in the evaluation of node trust value. A

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

highly mobile node will have little value of trust and stable nodes are trusted more. The detailed framework of proposed protocol is presented in section 3 and simulation analysis indicates that the proposed work shows significant improvement over the previous related work mentioned in the paper.

III. DESIGN OF PROPOSED PROTOCOL, DSNMR

This paper presents a novel security protocol called DSNMR which is applicable with on-demand routing approach. Basic versions of DSR and AODV discover multiple paths between source and destination nodes but they use only one path for data transfer. To experience the full benefits of multipath routing like load balancing and security, the routing protocol must use all existing distinct node-disjoint paths for data transfer. With this observation, our protocol DSNMR is designed to discover and use all possible distinct node-disjoint multiple paths between source and destination. Moreover, DSNMR discovers most secure and authenticated routes using asymmetric cryptographic scheme and the data transmission is secured with trust based scheme. Specifically, DSNMR calculates trust value of each node by considering packet drop ratio and remaining battery power.

A. Assumptions

While designing the proposed protocol DSNMR, it is assumed that there are 'n' number of nodes present in the MANET. Each node in MANET is capable of acting as both router and host. As there is no specific centralized node to monitor networking functionalities like routing, security, etc. each node takes care of itself. Often it is possible that source and destination hosts are separated by numerous intermediate nodes, and during data transfer between them, each node has to trust other nodes. The MANET uses on-demand routing scheme which finds routes between source and destination hosts only when there is data transfer between them and the routes are alive until all the data transmission is completed. On-demand routes are discovered using query-reply approach and it is assumed that only destination node gives route reply message and all other intermediate nodes do not reply but simply forward the route request. This is assumed so that all possible existing distinct node-disjoint multiple paths can be discovered between source and destination nodes. Specifically, the MANET uses node-disjoint multipath routing scheme for security reasons.

B. DSNMR Description

The proposed DSNMR protocol discovers all possible distinct node-disjoint on-demand multipath routes constrained to certain maximum hop count,through which the data can be transmitted from source to destination node. During routes discovery process, necessary security measurements are taken to avoid DoS attacks by malicious nodes. Also, all the intermediate nodes present between source and destination nodes are authenticated such that the security problems like man-in-the-middle attacks [43] can be prevented. Hence, DSNMR uses a simple light weight trust based secure mechanism to control the loss of data packets by such selfish nodes. During routes discovery process, DSNMR also calculates each route trust value as the sum of trust values of all the nodes in that route. DSNMR transmits the data according to the trust values of routes i.e. a route with higher trust value carries more number of data packets than a route with lower trust value. During data transmission, DSNMR periodically calculates each route trust value and accordingly data packets to be transmitted through those routes are determined. Any kind of trust based model can be included with the proposed secure route discovery process. This kind of general framework of DSNMR provides flexibility to experiment with different trust models.

As the first step, in DSNMR, all the nodes have to authenticate their one-hop neighbourhood nodes using asymmetric cryptography scheme. If n_i is a node 'i' then it can have a pair of public and private(secret) keys as $[PK_i, SK_i]$ respectively using asymmetric cryptography system [44]. All the nodes share their public key PK_i with other nodes through public key certificate $CERT_i$ issued by certificate authority. The key generation schemes and certificate authority schemes are beyond the scope of the paper and there are several such schemes as [45]–[47]. The certificate $CERT_i$ of node n_i also contains its unique identifier ID_i issued by certificate authority. The size of ID_i depends decides the maximum number of nodes that can present in MANET. For example, using a 2-byte ID_i, a maximum of 65,535 nodes can be addressed.

Each node n_i has to share its information in the form of $CERT_i$ with its one-hop neighbours by broadcasting a signed message Msg_i periodically. The structure of message Msg_i at time 't' is $< t, ID_i, sig_i(t, ID_i), CERT_i >$ where $sig_i(t, ID_i)$ is the digital signature of node n_i having identifier ID_i and signed at time 't'. All the nodes can verify their one-hop neighbours by verifying signatures of each other.The timeperiod for neighbourhood verification depends on system parameters such number of nodes, connectivity, topology changes, etc. Once the neighbourhood verification stage is over, each node n_i will have its one-hop neighbour list N_i at time t.

Once each node n_i has its one-hop authenticated neighbour list N_i, the route discovery process will be initiated by a source node S to the destination node D. Since our protocol DSNMR is designed to work with on-demand routing protocols, when a source node S has some

data to transfer to a destination node D, then node S first checks for route to D in its routing table. If no route is found to D, then node S composes a route-request message $RREQ_{S,D}$ as follows:

$$RREQ_{S,D} = < ID_S , ID_D \text{ ,SEQ, } HopCount_{current} , HopCount_{\max} , E_{PK_D}(Key_{S,D}) , List_{Route} , List_{Exclude} , Trust_{Route}, List_{NextHop} , hash_{Key_{S,D}}(ID_S, ID_D, SEQ, HopCount_{\max}) >$$

Here ID_S and ID_D are the identifiers of source node S and destination node D. SEQ is the unique sequence number generated for each new route request message so that duplicate messages can be discarded. Current hop count and maximum hop count are tracked using $HopCount_{current}$ and $HopCount_{\max}$ respectively. The value of $HopCount_{\max}$ is fixed by source node S based on current knowledge on network connectivity, node density, etc. and it is not modified by any other intermediate node present between S and D. But $HopCount_{current}$ value is incremented by 1 each time an intermediate node forwards $RREQ_{S,D}$. Initial value of $HopCount_{current}$ is 0 which is set by source node S. When $HopCount_{current}$ value reaches $HopCount_{\max}$, the route request message $RREQ_{S,D}$ cannot be forwarded by intermediate nodes. $Key_{S,D}$ is the sessional key shared by both source and destination nodes S and D respectively. The source node S randomly selects and encrypts the session key $Key_{S,D}$ using public key PK_D of destination node D such that D is the only node which can decrypt the $Key_{S,D}$ and the intermediate nodes cannot decrypt the $Key_{S,D}$ as it can be decrypted by only private key of node D which is not available with the intermediate nodes. $E_{PK_D}(Key_{S,D})$ is the encrypted session key used by both nodes S and D for secure data transmission. $List_{Route}$ is dynamically updated list by intermediate nodes that become the part route from S to D. Similarly, $List_{Exclude}$ is the dynamically generated list by the intermediate nodes present between S and D and this list specifies the nodes that are excluded from being part of route discovery of a particular thread of route request query. The two lists $List_{Route}$ and $List_{Exclude}$ are containing only ID_S and they are incrementally populated by intermediate nodes during route discovery process. $Trust_{Route}$ is the aggregated trust value of a route which is initiated by source node S. First, node S adds its trust value to $Trust_{Route}$ and then $Trust_{Route}$ is updated by each intermediate node that becomes the part of route. $List_{NextHop}$ is the list of nodes which is dynamically populated by intermediate nodes that become next hops of query. Static data like $(ID_S, ID_D, SEQ, HopCount_{\max})$ is hashed with session key $Key_{S,D}$ such that the data is not maliciously modified by intermediate nodes.

$hash_{Key_{S,D}}(ID_S, ID_D, SEQ, HopCount_{\max})$ is the hashed key function of static data $(ID_S, ID_D, SEQ, HopCount_{\max})$.

Each node n_i has a trust value at time 't' $Trust_i^t$ which is calculated as follows:

$$Trust_i^t = w_1 \frac{Pack\,\mathrm{Re}cd_i^t}{PackFwd_i^t} + w_2 RP_i^t + w_3 MI_i^t$$

where $Pack\,\mathrm{Re}cd_i^t$ is number of packets (both data and control packets) received by node n_i upto time 't' and $PackFwd_i^t$ is the number of packets forwarded by node n_i upto time 't'. The parameter RP_i^t indicates the remaining power of node n_i at time 't'.

The value of RP_i^t is calculated as follows:

$$RP_i^t = IE_i - EC_i^t$$

where IE_i is the initial energy of node n_i and EC_i^t is the energy consumed by n_i upto time 't' since the node is turned on. The value of EC_i^t is $EC_i^t = EC_r^t + EC_x^t$ where EC_r^t is the energy consumed on receiving packets upto time 't' and EC_x^t is the energy used to transmit the packets upto time 't'.

MI_i^t is the mobility index of node n_i at time 't'. Average distance covered by node n_i in a specific time period T is measured as

$$D(n_i^t) = \sqrt{(x(n_i^t) - x(n_i^{t-1}))^2 + (y(n_i^t) - y(n_i^{t-1}))^2}$$

where $(x(n_i^t), y(n_i^t))$ and $(x(n_i^{t-1}), y(n_i^{t-1}))$ are the coordinates of node n_i at time t and t-1 respectively.

Three weight parameters w1,w2 and w3 are used in trust calculation and the values are set according to network conditions and application requirements. If more secure path is required the weight of w1 can be increased or if a long lasting route is required then the weight of w2 can be increased or if stable nodes are needed in route then w3 value can be increased. In our simulations, we gave equal weights to all parameters.

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

When an intermediate node receives a $RREQ_{S,D}$ packet the node first hashes the packet and stores the hashed value in its routing table for some time. Meanwhile, if the same $RREQ_{S,D}$ packet is received, it will find the same hash value in its routing table and drops the packet. But if a different instance of $RREQ_{S,D}$ packet is received by the node then definitely its hashed value will be different because $List_{Route}$, $List_{Exclude}$ and $List_{NextHop}$ values are different. This way an intermediate node is not prevented from calculating different paths towards destination node D. All existing possible distinct node-disjoint multiple paths will be discovered. Since the proposed protocol DSNMR has to find node-disjoint paths, each intermediate node checks whether any common node is participating in two or more paths by checking $List_{Route}$ and $List_{Exclude}$. Also, when an intermediate node n_i receives a $RREQ_{S,D}$, it checks whether its identifier ID_i is present in received $List_{NextHop}$ and checks whether the node identifier from which $RREQ_{S,D}$ is received is the last one in the list $List_{Route}$ and belongs to its authenticated neighbours list N_i. If any one of these checks fail, the node n_i drops $RREQ_{S,D}$. If the node n_i processes $RREQ_{S,D}$ then it simply increases $HopCount_{current}$ by 1 and checks the new value crosses $HopCount_{\max}$. If so, the packet will be dropped, otherwise it will append its identifier ID_i to the $List_{Route}$ and forwards to its neighbours. The node n_i also updates the $List_{Exclude}$ by appending all the node identifiers present in the received $List_{NextHop}$ into $List_{Exclude}$ to eliminate duplicate processing of packet $RREQ_{S,D}$.

When the destination node D receives the $RREQ_{S,D}$, it decrypts $E_{PK_D}(Key_{S,D})$ with its private key SK_D and checks the validity of hashed value. Then node D waits for some time to receive different instances of $RREQ_{S,D}$ from different routes. Node D then constructs maximum set of node-disjoint paths and composes route reply message $RREP_{D,S}$ for each instance of $RREQ_{S,D}$ with different $List_{Route}$.

$RREP_{D,S}$ = < ID_S , ID_D , SEQ, $List_{Route}$, $Trust_{Route}$, $hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})$ >

When each intermediate node n_i receives $RREP_{D,S}$, it checks its identifier ID_i in $List_{Route}$. If not present, the node n_i drops the packet. Otherwise, it also checks the node identifiers of neighbours before and after its ID_i in $List_{Route}$ are in N_i. Then, node n_i rebroadcasts $RREP_{D,S}$ until it reaches the source node S. Finally, when $RREP_{D,S}$ reaches the source node S, it verifies the hash value of $hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})$. If it is valid, then $List_{Route}$ will be stored as valid path to reach destination node D. Once all the route replies from node D are received and node-disjoint paths are stored in the routing table, the source node S prioritizes the paths based on $Trust_{Route}$. If there are 'k' node-disjoint paths are present, then weight factors of paths to decide amount of data to be transmitted through paths are decided as follows;

$$W_i = \frac{Trust^i_{Route}}{\sum_{i=1tok} Trust^i_{Route}}$$

where W_i is the weight factor of 'ith' route and $Trust^i_{Route}$ is the $Trust_{Route}$ value of 'ith' route.

The source node S transmits the data through different multiple node-disjoint paths based on the trust values of routes. Periodically, the node S recalculates the weights of routes according to their dynamic $Trust_{Route}$ values.

C. DSNMR Algorithm

Input: Each node n_i in MANET has:

- a pair of keys $[PK_i, SK_i]$
- unique identifier ID_i
- certificate $CERT_i$ issued by certificate authority

/ authenticating one-hop neighbors */*

1. Each node n_i broadcasts periodically Msg_i

$< t, ID_i, sig_i(t, ID_i), CERT_i >$

2. Each node n_i builds one-hop neighbour list N_i at time t

/ at source node */*

3. Source node S issues route request query:

$RREQ_{S,D}$ = < ID_S , ID_D , SEQ, $HopCount_{current}$, $HopCount_{\max}$, $E_{PK_D}(Key_{S,D})$, $List_{Route}$, $List_{Exclude}$, $Trust_{Route}$, $List_{NextHop}$, $hash_{Key_{S,D}}(ID_S, ID_D, SEQ, HopCount_{\max})$ >

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

/ at each intermediate node */*

4. Each intermediate node n_i hashes the received route request query packet and stores the hashed value of first query packet in its routing table.
$hash_{Key_{S,D}}(RREQ_{S,D})$

5. if $hash_{Key_{S,D}}(RREQ_{S,D})$ value already present, then

6. drop $RREQ_{S,D}$

7. else update $List_{Route}$, $List_{Exclude}$ and $Trust_{Route}$

8. increment $HopCount_{current}$ by 1

9. if ($HopCount_{current} == HopCount_{\max}$) then

10. drop $RREQ_{S,D}$

11. else forward $RREQ_{S,D}$

/ at destination node */*

12. for each received $RREQ_{S,D}$, the destination node finds the hashed value as: $hash_{Key_{S,D}}(RREQ_{S,D})$

13. destination node stores all $RREQ_{S,D}$ with different $hash_{Key_{S,D}}(RREQ_{S,D})$ values

14. compose and broadcasts route reply message as:
$RREP_{D,S}$ = < ID_S , ID_D , SEQ, $List_{Route}$, $Trust_{Route}$, $hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})$ >

/* at each intermediate node */

15. Each intermediate node n_i checks $RREP_{D,S}$ as:

16. if (ID_i is in $List_{Route}$ or neighbours ID_i before and after its ID_i in $List_{Route}$ are in N_i) then

17. broadcasts $RREP_{D,S}$

18. else drop $RREP_{D,S}$

/* at source node */

19. for each received $RREP_{D,S}$, source node finds hashed key value as:
$hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})$

20. if ($hash_{Key_{S,D}}(ID_S, ID_D, SEQ, List_{Route})$) not valid

21. drop $RREP_{D,S}$

22. else store $List_{Route}$ in its routing table.

23. For each $List_{Route}$ in its routing table, source node S periodically calculates route trust value factor as:

$$W_i = \frac{Trust^i_{Route}}{\sum_{i=1 to k} Trust^i_{Route}}$$

24. Source node S determines and transmits amount of data through each $List_{Route}$ according to its W_i

25. Repeat steps 23 and 24 until entire data is transmitted.

IV. SIMULATION ANALYSIS OFDSNMR PROTOCOL

The performance of proposed protocol DSNMR is analysed using NS2 simulator [48] which is a discrete-event simulator used widely by networking academic research community people. The simulated model of MANET with 50 nodes distributed randomly in an area of 1000 m X 1000 m. Node propagation range is 250m and data transmission rate is 2m/s.

Random way point mobility model is considered to simulate the mobility behaviour of nodes. According to this model, a node randomly selects a destination node and then moves towards it with a random speed. After reaching the destination node, the node waits for certain pause time and then again, the node selects another random destination node and moves towards it with random speed. This way node mobility is simulated according to this model. In our simulation model, the node pause times are fixed as 0, 5, 10, 20, 30 and 40s. Pause time 0 means the nodes are continuously moving and pause time 40 means the nodes are stationary.

In our simulation runs, we selected randomly 10 pairs of source and destination nodes. The application data to be transmitted from source to destination is generated by traffic application CBR (Constant Bit Rate) with packet size 512 bytes. The simulation is conducted for 350s of simulation time. The medium access control protocol used in the simulation is IEEE 802.11 Distributed Coordination Function (DCF). During the discovery of node-disjoint multiple paths, we made destination node to wait for 5s to receive distinct route request messages and reply them. The simulations are run with various traffic scenarios with different interpacket times and for each scenario, ten movement patterns are considered. Our simulations used free space radio model.

Since our secure protocol DSNMR is inspired from the previous work [41], [42], simulation results of DSNMR are compared with that work.

Inspite of many security measures, it is difficult to detect selfish nodes that are dropping data packets at critical time. These selfish nodes participate in route discovery and become the part of path but they drop the data packets to save their battery power. Our protocol DSNMR takes care of such selfish nodes by considering trust values of nodes in the path. Average throughput of all communicating pairs in MANET is calculated by increasing the number of misbehaving nodes and the results are shown in Fig. 2. It is observed from the results

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

that DSNMR performs better than SecMR [41] and protocol [42] because they do not consider selfish node attacks. SecMR is not addressing any kind of data security other than the discovery of secured multiple node-disjoint paths. The protocol [42] discovers trust worthy routes and data is then encrypted and transmitted through paths and no protection for data drop. But our protocol DSNMR is focused in both issues of secure route discovery and dropping of data packets. Hence DSNMR is giving more throughput than others. Similarly, average end-to-end latency is also measured as it is an important metric of network performance and it is shown in Fig.3. DSNMR is better in end-to-end delay compared to other work SecMR and [42]. Usually, there is a trade-off between security overhead and network delay. But our DSNMR is providing security with significant delay since it is using simple trust model and path trust is calculated periodically as the part of route maintenance. In [42], the data is transmitted through multiple paths by encrypting each packet, hence it is taking more time than DSNMR.

Since node mobility is affecting network topology and thereby routing paths, we also measured network throughput with respect to node speed. Fig. 4 shows the result of network throughput with respect to node mobility.DSNMR gives better results than [42] as the route discovery process includes authenticating neighbourhood and also exclude list is used to avoid the nodes that could present in multiple paths. When a node moves away from path, it will be listed in exclude list and thereby path will be modified hence it results in high throughput than [42] where such list is not present. Moreover, trust value computation involves node mobility index which is discarded in [42].

Another important metric of packet drop percentage is also considered for the performance analysis of DSNMR and the results are shown in Fig. 5. DSNMR has the least percentage of data packet drop compared to SecMR and [42] where packet drop by malicious nodes is not considered.

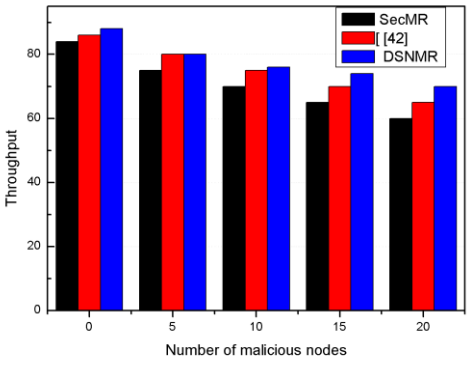

Fig. 2 Network throughput vs malicious nodes

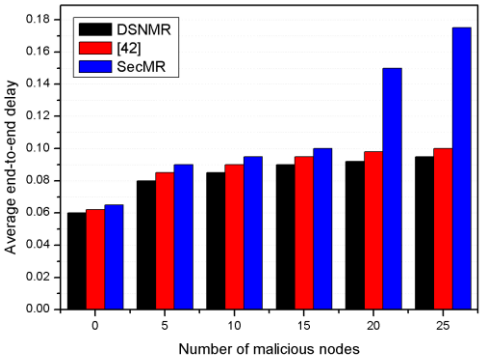

Fig. 3Average delayvs malicious nodes

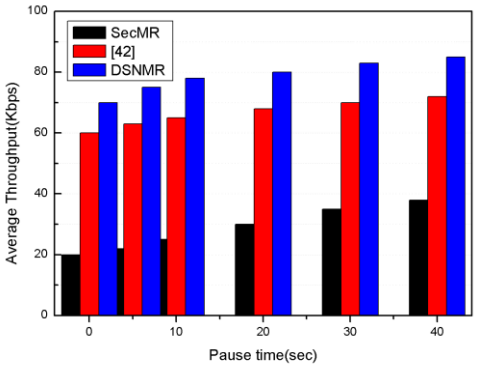

Fig. 4 Average throughput vs node mobility

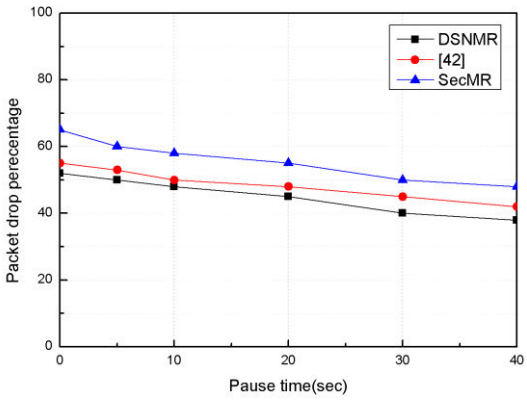

Fig. 5 Average packet drop percentage vs node mobility

V. CONCLUSIONS

Routing security and Data security are two important challenges in MANET research area. This paper proposes a new method DSNMR of providing both routing security and data security making use of on-demand node-disjoint multipath routing scheme where asymmetric cryptography

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

and trust-based security concepts are applied. In DSNMR, a complete set of node-disjoint multiple paths which are authenticated and reliable trusted paths are discovered. Also, node trust value computations involve the remaining battery power level so that energy efficient or selfish node free routes can be established. The amount of data to be transmitted through each path is determined in proportion to route trust value which is computed during route discovery process and route trust value is updated periodically during route maintenance. The node-disjoint loop-free secured multiple paths are discovered using asymmetric cryptography authentication principle and trust-based security model is used to prevent attacks from selfish nodes which may drop data packets during critical times of network operation. Moreover, unlike previous work, DSNMR considers node mobility index in the estimation of node trust value. The general framework of DSNMR can be experimented with suitable node-authentication scheme during route discovery and it is then combined with any reliable trust-based security model. The simulation results of DSNMRshows the significant performance compared to previous related work.

REFERENCES

[1] M Conti and S. Giordano, "Mobile ad hoc networking: Milestones, challenges, and new research directions," *IEEE Communications Magazine*, 2014.

[2] M. Conti *et al.*, "From MANET to people-centric networking: Milestones and open research challenges," *Computer Communications*, 2015.

[3] J. Loo, J. L. Mauri, J. H. Ortiz, and D. A. Maltz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. 2016.

[4] G. V. Kumar, Y. V. Reddyr, and M. Nagendra, "Current Research Work on Routing Protocols for MANET : A Literature Survey," *International Journal on Computer Science and Engineering*, 2010.

[5] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, 2004.

[6] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications*, 1996.

[7] C.-C. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "ROUTING IN CLUSTERED MULTIHOP, MOBILE WIRELESS NETWORKS WITH FADING CHANNEL," in *Proc. IEEE SICON*, 1997.

[8] T. W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad-hoc wireless networks," in *International Conference on Communications - Proceedings*, 1998.

[9] C. K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," *IEEE Communications Magazine*, 2001.

[10] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," 2002.

[11] D. B. Johnson and D. A. Maltz, "DSR : The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," *Computer Science Department, Carnegie Mellon University, Addison-Wesley*, 2001.

[12] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings - WMCSA'99: 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999.

[13] IETF, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," *Draft-Ietf-Manet-Zone-Zrp-04*, 2002.

[14] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012*, 2011.

[15] P. Goyal, S. Batra, and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks," *International Journal of Computer Applications*, 2010.

[16] A. Dorri and S. R. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey," *International Journal of Computer Science & Engineering Survey*, 2015.

[17] S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks," in *Procedia Computer Science*, 2016.

[18] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," *Ad Hoc Networks*, 2003.

[19] J. Liu, F. Fu, J. Xiao, and Y. Lu, "Secure routing for mobile ad hoc networks," in *Proceedings - SNPD 2007: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007.

[20] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, 2002.

[21] X. Huang and Y. Fang, "Performance study of node-disjoint multipath routing in vehicular Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, 2009.

[22] L. Liu and L. Cuthbert, "A novel QoS in node-disjoint routing for ad hoc networks," in *IEEE International Conference on Communications*, 2008.

[23] Xuefei Li and L. Cuthbert, "On-demand node-disjoint multipath routing in wireless ad hoc networks," 2004.

[24] J. Cai and W. Wu, "Degraded link-disjoint multipath routing in ad hoc networks," in *2009 4th International Symposium on Wireless and Pervasive Computing, ISWPC 2009*, 2009.

[25] J. Yi, A. Adnane, S. David, and B. Parrein, "Multipath optimized link state routing for mobile ad hoc networks," *Ad Hoc Networks*, 2010.

[26] B. Vaidya, J. Y. Pyun, S. Pan, and N. Y. Ko, "Secure framework for integrated multipath MANET with internet," in *Proceedings - 2008 International Symposium on Applications and the Internet, SAINT 2008*, 2008.

[27] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," in *2010 International Conference on*

Volume: 10 Issue: 05 Pages: 3990-3998 (2019) ISSN: 0975-0290

Measuring Technology and Mechatronics Automation, ICMTMA 2010, 2010.
[28] B. Vaidya, J. Y. Pyun, J. A. Park, and S. J. Han, "Secure multipath routing scheme for mobile ad hoc network," in *Proceedings - DASC 2007: Third IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 2007.
[29] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," *Wireless Networks*, 2017.
[30] X. Li, Z. Jia, P. Zhang, and H. Wang, "A trust-based multipath routing framework for mobile ad hoc networks," in *Proceedings - 2010 7th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2010*, 2010.
[31] B. Vaidya, D. Y. Choi, J. A. Park, and S. J. Han, "Investigation of secure framework for multipath MANET," *International Journal of Security and its Applications*, 2008.
[32] S. Berton, H. Yin, C. Lin, and G. Min, "Secure, Disjoint, Multipath Source Routing Protocol(SDMSR) for Mobile Ad-hoc Networks," in *Proceedings - Fifth International Conference on Grid and Cooperative Computing, GCC 2006*, 2006.
[33] S. Geetha and G. G. Ramani, "Trust based secure multipath OLSR routing protocol in MANET using fuzzy theory," 2012.
[34] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in *Proceedings - IEEE INFOCOM*, 2004.
[35] S. Adibi and S. Erfani, "A multipath routing survey for mobile ad-hoc networks," in *2006 3rd IEEE Consumer Communications and Networking Conference, CCNC 2006*, 2006.
[36] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *Proceedings - UKSim 15th International Conference on Computer Modelling and Simulation, UKSim 2013*, 2013.
[37] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris, "Secure multipath routing for mobile ad hoc networks," in *2nd Annual Conference on Wireless On-Demand Network Systems and Services, WONS 2005*, 2004.
[38] Y. V. Reddy and M. Nagendra, "A Study on Multipath Routing Security Protocols for Mobile Ad Hoc Networks," *International Journal of Computer Sciences and Engineering*, vol. 5, no. 12, pp. 243–248, 2018.
[39] P. P. and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference ({CNDS 2002})*, 2002.
[40] M. Burmester and T. Van Le, "Secure multipath communication in mobile ad hoc networks," in *International Conference on Information Technology: Coding Computing, ITCC*, 2004.
[41] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR - a secure multipath routing protocol for ad hoc networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 87–99, Jan. 2007.
[42] P. Gera, K. Garg, and M. Misra, "Trust-based multi-path routing for enhancing data security in MANETs," *International Journal of Network Security*, 2014.
[43] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J. J. Quisquater, "Secure implementation of identification systems," *Journal of Cryptology*, 1991.
[44] N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," in *Towards a Quarter-Century of Public Key Cryptography*, 2013.
[45] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," 2003.
[46] S. Yi and R. Kravets, "MOCA : MObile Certificate Authority for Wireless Ad Hoc Networks," in *Proceedings of the 2nd Annual PKI Research Workshop (PKI '03)*, 2003.
[47] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, 1999.
[48] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*. 2012.
[49] Periyasamy, P., and E. Karthikeyan. "A simulation based QoS review of multipath routing protocols for MANET." International Journal of Advanced Networking and Applications 4.3 (2012): 1624.